


Intel ME

Минко В.



О себе



- ИнфоТеКС — российский разработчик программно-аппаратных VPN-решений и СКЗИ. Выпускает продукты ViPNet.
- Системный архитектор, отдел ПиР ПАК.
- Проекты ПАК HW и ПАК xFirewall.



2

©2017, ОАО «ИнфоТеКС»

Для начала я хочу рассказать немного о себе.

Я работаю в компании ИнфоТеКС (Информационные Технологии и Коммуникационные Системы). Это российский разработчик программно-аппаратных VPN-решений и СКЗИ. Выпускает продукты под брендом ViPNet.

Я работаю в компании на позиции системного архитектора в отделе ПиР ПАК.

По своей работе я занимаюсь проектированием программно-аппаратных комплексов HW и xFirewall. Это криптошлюз и межсетевой экран нового поколения (NGFW).

В сферу моих интересов попадают и вопросы безопасности этих ПАК-ов.

Материалы доклада – это открытые источники, а не какие-то мои личные исследования. В основном это доклады конференций и статьи.

План доклада

infotecs

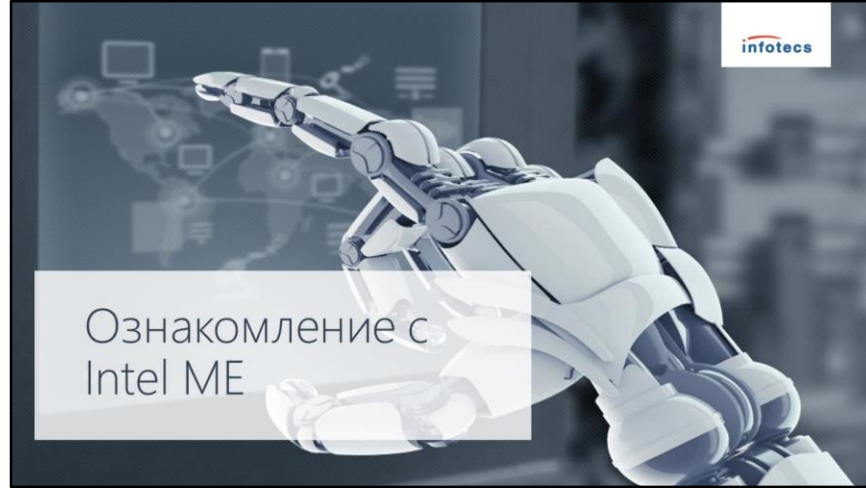
- Ознакомление с Intel ME.
- Архитектура Intel ME.
- Технологии на основе Intel ME.
- Способы отключения Intel ME.
- Вопросы и ответы.



3

©2017, ОАО «ИнфоТекс»


Доклад разделён на три следующие части.



Ознакомление с
Intel ME

infotecs

AMT 1.0 и его возможности



Active Management Technology - решение для удалённого администрирования.
Основывается на интегрированном в чипсет микроконтроллере (Management Engine).

- Внеполосный (out-of-band) доступ к сетевому интерфейсу.
- Внутренний веб-сервер с TLS-шифрованием.
- Доступ к периферийному оборудованию (в т.ч. к клавиатуре).
- Микроконтроллер начинает работать при подаче питания на материнскую плату (т.е. даже когда машина выключена).

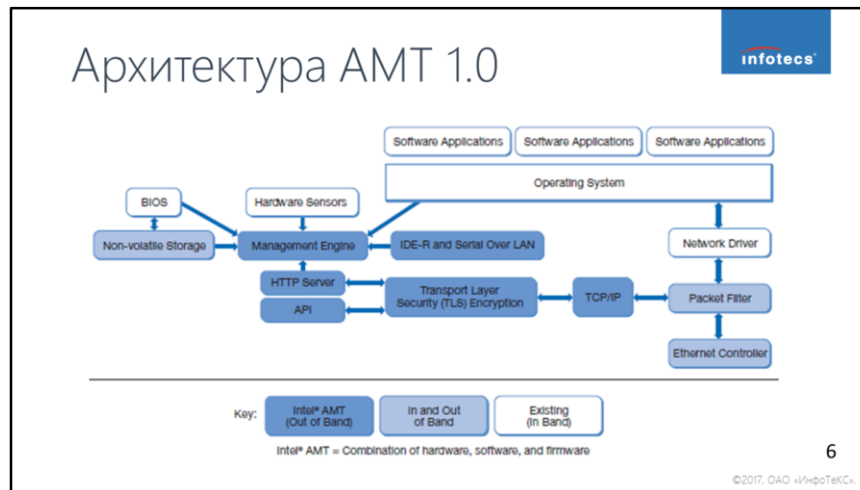
5

©2017, ОАО «ИнфоТекС»

В 2005 году компания Intel представила Active Management Technology (AMT) версии 1.0 — решение для удалённого администрирования (управление, инвентаризация, обновление, диагностика, устранение неполадок и т.д.).

Архитектура AMT 1.0 основывается на интегрированном в чипсет микроконтроллере (Management Engine), наделённому весьма впечатляющими возможностями, например:

- внеполосный (out-of-band) доступ к сетевому интерфейсу (Ethernet), который он разделяет с основным CPU;
- внутренний веб-сервер с TLS-шифрованием (для администрирования);
- доступ к периферийному оборудованию, получение и хранение в энергонезависимой памяти информации о нём;
- микроконтроллер начинает работать при подаче питания на материнскую плату компьютерной системы (т.е. при подключении компьютера к электрической сети, ещё до того, как пользователь нажмёт кнопку Power).



Если мы взглянем на архитектуру Active Management Technology 1.0, мы увидим как реализован внеполосный доступ к сетевым интерфейсам.

На схеме присутствует микроконтроллер Management Engine, который связан с разными подсистемами: OS, BIOS, SPI.

ME имеет собственный контроллер канального уровня, осуществляет мониторинг всего входящего сетевого трафика, из которого «вырезает» (при помощи Packet Filter) пакеты, предназначенные для него. Для ОС (наличие и состояние которой на работу AMT никак не влияет) этот трафик уже не виден;

AMT 2.0, ME 2.0

infotecs

- Первые версии ME относились непосредственно к AMT, нумерация достаточно условная.
- 2006г – выход AMT 2.0, появление бренда vPro, подсистему наименовали в Intel Management Engine (ME) версии 2.0.

7

©2017, ОАО «ИнфоТекс»

Первые версии ME не имели, собственно, такого названия (“Intel ME”), потому нумерация их достаточно условна (т.к. это относилось к AMT) и приведено больше чисто для хронологии.

В 2006-м году с выходом AMT версии 2.0. Именно тогда подсистему наименовали в Intel Management Engine (ME) версии 2.0.

Одновременно с этим появился бренд Intel vPro, который обозначал комплекс реализованных на основе Intel ME технологий: AMT, Позже в этот список вошли Identity Protection Technology (IPT) и Anti-Theft (AT).
??Trusted Execution Technology (TXT) и Virtualization Technology (VT)

Современный Intel ME

infotecs

ME: High-level overview

- Management Engine (or Manageability Engine) is a dedicated microcontroller on all recent Intel platforms
- In first versions it was included in the network card, later moved into the chipset (GMCH, then PCH, then MCH)
- Shares flash with the BIOS but is completely independent from the main CPU
- Can be active even when the system is hibernating or turned off (but connected to mains)
- Has a dedicated connection to the network interface; can intercept or send any data without main CPU's knowledge

I. Skochinsky: Secret of Intel Management Engine

(c) 2014 Igor Skochinsky

4

8

©2017, ОАО «ИнфоТекС»

С тех пор ME непрерывно развивался. Брал на себя новые функции и получал новые возможности. Современный ME (точнее на 2014-й год) достаточно подробно исследовал и описал Игорь Скочинский, результаты его работы легко доступны в сети. Доклад называется: Secret of Intel Management Engine

Современный Intel ME

infotecs

- Добавлен полный доступ на чтение и запись ко всему содержимому оперативной памяти (доступ разделяется с CPU).
- Добавлена возможность захвата видеопотока (только при использовании интегрированной графической подсистемы Intel).
- Добавлена возможность получать Java-bytecode через сеть и исполнять его.

<https://github.com/skochinsky/me-tools>

9

©2017, ОАО «ИнфоТекс»

В частности, Скочинский описывает следующие возможности:

- Добавлен полный доступ на чтение и запись ко всему содержимому оперативной памяти (доступ разделяется с CPU).
- Добавлена возможность захвата видеопотока (только при использовании интегрированной графической подсистемы Intel). Что позволило реализовать такие функции как KVM.
- Добавлена возможность получать Java-bytecode через сеть и исполнять его.

Утилиты для анализа прошивки, написанные Игорем опубликованы на github:

<https://github.com/skochinsky/me-tools>

Наличие Intel ME

infotecs

- Настольные и мобильные GMCH: Q965, Q35, Q45 и мобильные.
- Настольные и мобильные PCH: 5-9, 100 series.
- В серверных платформах как Intel Server Platform Services.
- Позднее появилась и в System-on-a-Chip (Intel Trusted Execution Engine).
- Сейчас каждая современная мобильная/настольная/серверная машина Intel включает в себя подсистему Intel ME.

10

©2017, ОАО «ИнфоТекс»

Из-за высокой стоимости реализации, изначально эта подсистема присутствовала, за несколькими исключениями, только на материнских платах с чипсетами Intel линейки Q.
Q965 / GM965 / GME965 / GL960 / GLE960 / PM965 / Q35 / GM45 / PM45 / Q45 (Graphics and Memory Controller Hub).
Начиная с 2010 года, подсистему Intel ME стали встраивать во все чипсеты производства Intel (Platform Controller Hub).




Архитектура Intel ME

Теперь предлагаю немного погрузиться в технические подробности и узнать как устроена подсистема ME. Это поможет нам в том числе и для понимания последней части доклада – способов отключения ME.



Начиная с 2010 года, вместе с переносом части функциональных блоков северного моста (графическое ядро, контроллер памяти, ...) в корпус CPU, ME-контроллер остался в корпусе чипсета – в Platform Controller Hub (PCH). Это чипсеты 5 серии и выше.

Микроконтроллеры ME



- ME 1.x-5.x – основан на микропроцессоре ARCtangent-A4.
- ME 6.x-10.x – на ARCtangent-A5/ARC600.
- ME 11.x (Skylake, PCH 100) – на x86.
- В Intel SoC – SPARC.

14

©2017, ОАО «ИнфоТекс»


В двухкорпусных чипсетах Intel в качестве базовой модели ME-контроллера использовался ARCtangent-A4 со стандартной системой команд ARC32.

В однокорпусных чипсетах уже использовались ARCtangent-A5/ARC600 с компактной системой команд ARCcompact (ARC16/32).

в самых последних платформах (Skylake, чипсеты 100 серии, Intel ME 11.x) ME-контроллер имеет архитектуру... x86!

В Intel SoC (там где эта подсистема называется Intel TXE) в качестве базовой модели для ME-контроллера используется SPARC.

Состав подсистемы Intel ME



- ME-контроллер
- Регион флэш-памяти SPI
- ME UMA
- Management Engine Interface
- MAC
- Модули в BIOS

15

©2017, ОАО «ИнфоТекС»

Состав компонентов подсистемы Intel ME не менялся с версии 2.0. Рассмотрим его:

ME-контроллер – встроенный в чипсет микроконтроллер на основе микропроцессора одной из рассмотренных выше архитектур;

Регион ME в SPI флэш-памяти, в котором хранится разработанная и подписанная компанией Intel прошивка ME-контроллера;

ME UMA – скрытая ото всех, кроме ME-контроллера, область (16 — 32 МБ) в оперативной памяти компьютера, которой он пользуется в качестве runtime-memory для размещения и запуска прошивки;

Management Engine Interface (MEI), ранее известный как **Host Embedded Controller Interface (HECI)** – представляет собой интерфейс для обмена информацией с ME-контроллером (по сути, единственный канал связи софта, исполняющегося на CPU, с подсистемой Intel ME);

Отдельный MAC – контроллер канального уровня, предоставляющий ME-контроллеру out-of-band доступ к общему физическому сетевому интерфейсу для удалённого администрирования компьютерной системой;

Некоторые модули в BIOS, отвечающие за инициализацию платформы и сообщающие о результатах своей работы ME-контроллеру через MEI.



Внутри ME-контроллера, помимо микропроцессора ARC/SPARC/x86:

- ME ROM – энергонезависимая неперезаписываемая память, в которой хранится стартовый код ME-контроллера и некоторая другая информация;
- ME SRAM – оперативная память используемая ME-контроллером при недоступности ME UMA, например, на ранних этапах работы;
- кэш кода и кэш данных, для повышения производительности при работе с памятью;
- C-Link (Controller Link) – шина, позволяющая ME-контроллеру взаимодействовать с периферийным аппаратным обеспечением в режимах S5 (System shutdown) / S3 (Sleep mode);
- Различные аппаратные блоки:
 - высокоточный таймер и WDT;
 - контроллер прерываний;
 - контроллеры памяти и DMA;
 - интерфейс HECI/MEI;
 - RNG, акселератор криптографических функций и функций сжатия.

SPI-регион Intel ME

The diagram shows a vertical stack of four regions in the SPI-Region Intel ME:

- BIOS Region 1 (top, light red)
- Intel ME Region 2 (second from top, blue)
- GbE Region 3 (third from top, yellow)
- Flash Descriptor Region 0 (bottom, blue)

Arrows on the right point to each region, indicating they are part of the firmware structure.

- Два типа ME firmware:
1.5 МБ (урезанные версии), 5.0 МБ (полные версии).
- Тип прошивки определяет состав прикладных модулей.

17
©2017, ОАО «ИнфоТекс»

Как было сказано ранее, в подсистему ME входит регион SPI-памяти, в котором и хранится прошивка Intel ME.

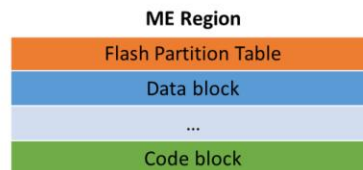
В зависимости от наполнения, различают два типа прошивок:

- 1.5 МБ, урезанные версии;
- 5 МБ, полные версии.

Тип прошивки определяет состав прикладных модулей, в которых реализованы определённые технологии (например, AMT, IPT и т.д.). Хотя есть и базовая часть, одинаковая для разных прошивок:

- Bring Up, первый запускаемый модуль из прошивки;
- Kernel, ядро OSCP ThreadX;
- Некоторые драйверы и службы.

Структура SPI-региона ME



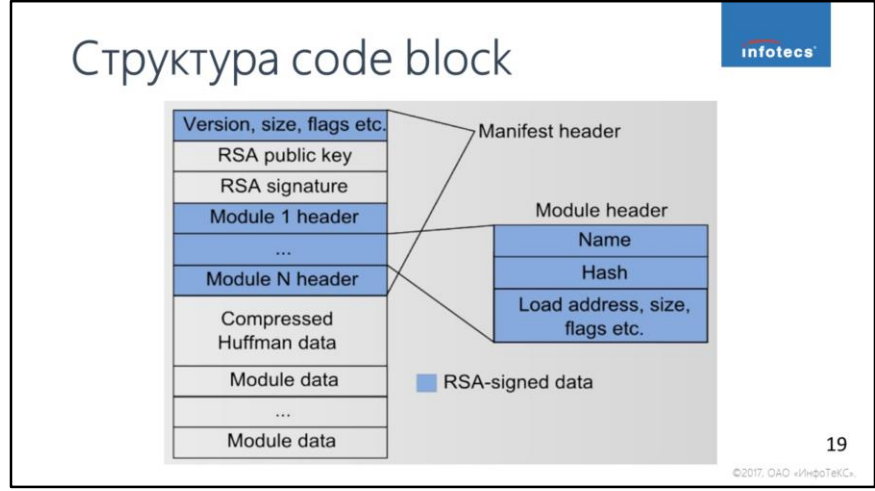
18

©2017, ОАО «ИнфоТекс»

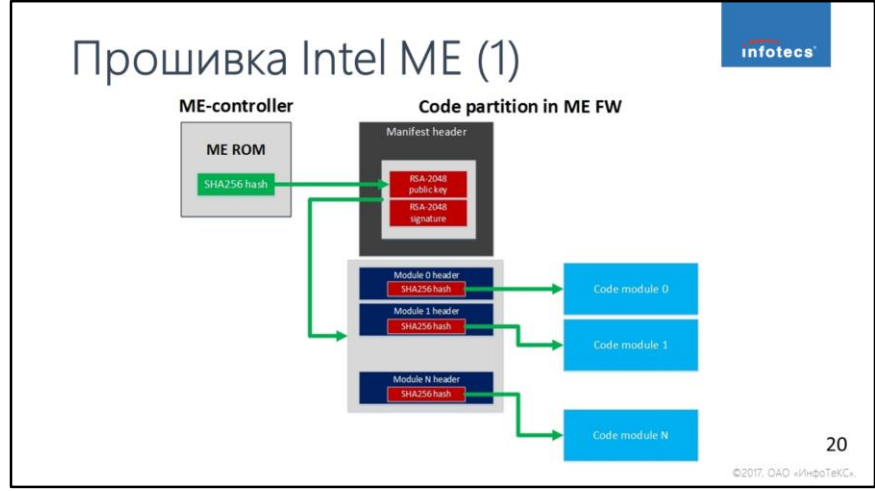
Структура региона ME сама по себе не монолитна.

В начале идёт таблица разделов (Flash Partition Table). В ней хранятся указатели на различного типа разделы (код, данные, виртуальная область, ...) и их параметры.

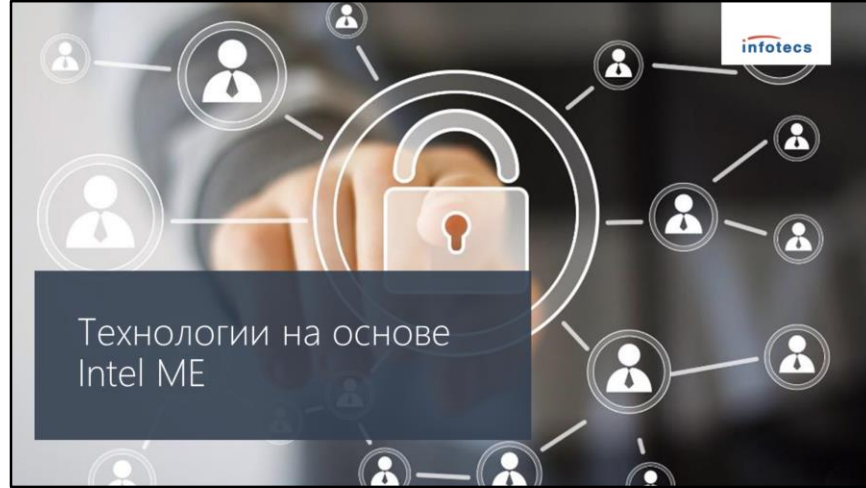
Нас интересуют исполнимые раздел, т.е. те, что хранят исполнимый код.




В начале кодового раздела располагается манифест, который состоит из заголовка (со служебными данными и ЭЦП) и таблицы модулей. Своим закрытым ключом компания Intel подписывает часть заголовка манифеста и таблицу модулей, прикладывая полученную подпись и открытый ключ для проверки. Сгенерировать собственную пару ключей RSA-2048 и подписать ими раздел не получится ввиду того, что целостность приложенного открытого ключа проверяется стартовым кодом в ME ROM, в котором хранится хеш-сумма SHA256 открытого ключа компании Intel.



В итоге, схему верификации кодового раздела ME firmware можно обобщить на рисунке. Каждый кодовый раздел верифицируется по этой схеме. Этого более чем достаточно для защиты прошивки от подделывания. Программно перезаписать ME регион SPI флеш-памяти нельзя, аппаратные средства, конечно позволят обойти это ограничение, но контроль подлинности не выключить.



Технологии на основе ME



- Active Management Technology
- Anti-Theft Technology
- Identity Protection Technology

22

©2017, ОАО «ИнфоТекС»

Переходим к рассмотрению технологий, основанных на ME.

- Сперва мы рассмотрим подробнее **Active Management Technology**.

Эта технология, с которого началась история ME и до сих пор, пожалуй, остаётся основной и наиболее востребованной технологии, реализованной на базе ME. Однако, были созданы и некоторые другие интересные технологии Intel на базе ME, которые, однако, оказались менее востребованными. Мы остановимся на следующих:

- **Anti-Theft Technology**
- **Identity Protection Technology**

Технологии на основе ME



- Active Management Technology
- Anti-Theft Technology
- Identity Protection Technology

23

©2017, ОАО «ИнфоТекс»

Начнём с более подробного рассмотрения AMT

Active Management Technology

Аппаратная технология для удалённого управления компьютером.

- **Включение, выключение, перезагрузка** (всё вне зависимости от состояния компьютера)
- **Serial-over-LAN** - виртуальный последовательный порт по сети
- **IDE Redirection** — перенаправление (по сети) загрузки с локальных носителей на предварительно сконфигурированный образ
- **Удалённая инвентаризация** аппаратуры

24
©2017, ОАО «ИнфоТекС»

Active Mangement Technology – это аппаратная технология для удалённого управления компьютером. AMT первой версии обладал следующим функционалом:

- **Включение, выключение, перезагрузка** (всё вне зависимости от состояния компьютера)
- **Serial-over-LAN** - виртуальный последовательный порт по сети, который позволяет удалённо производить (относительно простые) действия (например, настраивать BIOS Setup)
- **IDE Redirection** — перенаправление (по сети) загрузки с локальных носителей на предварительно сконфигурированный образ, позволяющий с него загрузиться (в отличие от PXE — не требуется наличие DHCP-сервера, сконфигурированного специально под это)
- **Удалённая инвентаризация** аппаратуры (т.е. получение данных о составе «железа»)

Active Management Technology

Позднее были добавлены:

- **System Defense** - технология для борьбы с вирусами, блокирует сеть при подозрительной сетевой активности
- **Agent Presence** - позволяет ставить на «аппаратное слежение» наличие выбранного процесса в ОС
- Поддержка работы по WiFi
- **CIRA** - канал связи между AMT и администратором создаётся по инициативе AMT-компьютера через промежуточный прокси-сервер
- **KVM** - удалённое управление компьютером в графическом режиме


25
©2017, ОАО «ИнфоТекС»

За 10 с лишним лет существования технология AMT непрерывно развивалась. В частности в неё были добавлены следующие функции, которые я хотел бы отметить:

- **System Defense** – технология для борьбы с вирусами. Позволяет задавать правила работы сетевой карты. Система автоматически считает количество исходящих запросов на открытие соединений в единицу времени. При превышении заданного порога, сеть блокируется. В то же время канал связи AMT продолжает работать, позволяя после устранения проблемы "разблокировать" (удалённо) систему, "вернув" ей доступ в сеть. System Defense появилась в AMT 2.0.
- **Agent Presence** – позволяет ставить на «аппаратное слежение» наличие выбранного процесса в ОС. Когда процесс по любой причине исчезнет (например, был остановлен антивирус вражеским процессом вируса) - админу по "AMT-каналу" отправлялось соответствующее предупреждение. Администратор сможет сразу предпринять какие-то действия. Agent Presence появилась в AMT 2.0.

- Поддержка работы АМТ по **WiFi**
- Возможность работы через интернет с помощью **CIRA** (Client Initiated Remote Access) - когда канал связи между АМТ и администратором создавался путём "вызова" со стороны АМТ-компьютера, что позволяло соединиться с АМТ-компьютером, стоящим за МЭ. Технология работает следующим образом: АМТ-компьютер "инициирует соединение" с прокси-сервером (Management Proxy Server). Админ со своей Management-консоли может подключить к MPS-серверу и получать, либо отправлять данные на АМТ-компьютер через MPS. Канал АМТ-MPS обычно использует TLS-шифрование.
- В версии АМТ 6.0 появилась поддержка **KVM** (Keyboard Video Mouse) - удалённое управление компьютером в графическом режиме, причём сеанс работы не прекращается даже в момент перезагрузки. В последних версиях АМТ разрешение поддерживается до 2560x1600.

Конфигурация АМТ



Процесс конфигурации АМТ можно разделить на два отдельных процесса:

1. Инициализация (Provisioning, Initialization)
2. Настройка (Configuration, Setup)

26

©2017, ОАО «ИнфоТекс»

Процесс конфигурации АМТ можно разделить на два отдельных процесса:

1. сначала проходит процесс "первичной" инициализации (однократно),
2. после может быть сколько угодно процессов настройки АМТ.

В документации есть некоторая путаница с терминологией и бывает, что используются разные названия для этих процессов.

Способы инициализации АМТ

- Ручная инициализация через MEBx
- Инициализация через PID+PPS (Provision ID, PreProvision Secret)
- Инициализация через USB
- Инициализация через Internet (Bare Metal)

27

©2017, ОАО «ИнфоТекс»

Инициализация предназначена для ответа на вопрос «как администратору получит доступ к АМТ в самый первый раз?»

Поставить какой-то простой логин-пароль, аналогично тому, как такое делается, к примеру, для роутеров - нельзя, ведь тогда любой сможет получить управление над не успевшими (забытыми) изменить пароль по умолчанию.

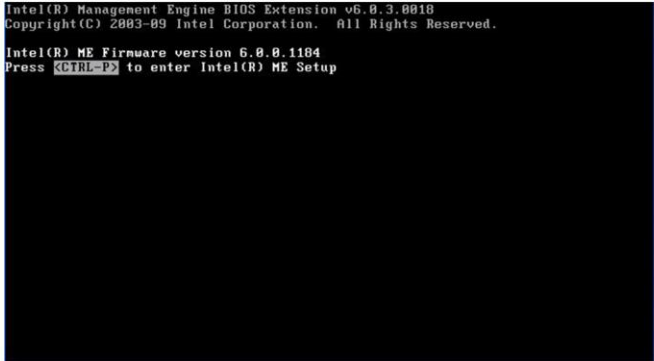
Включение AMT в BIOS



The screenshot shows the 'ThinkPad Setup' BIOS interface. At the top, there is a 'Config' tab. The main menu is titled 'Intel (R) AMT'. Below this, the 'Intel (R) AMT Control' is set to '(Enabled)'. Other options listed are 'CIRA Timeout' with a value of '[0]' and 'Console Type' with a value of '[UT100-]'. To the right of the settings is an 'Item Specific Help' section containing the text: 'This option enables or disables Intel (R) Active Management Technology (AMT) function. Select Enabled to start configuring the functions.' At the bottom of the screen, there is a navigation bar with the following key functions: F1 Help, T1 Select Item +/- Change Values, F9 Setup Defaults, Esc Exit, ← Select Menu, Enter Select ► Sub-Menu, and F10 Save and Exit. The number '28' is displayed in the bottom right corner of the screenshot area.

В любом случае инициализации необходимо, чтобы AMT была включена в BIOS. Состояние по умолчанию может зависеть от вендора компьютера. В случае с Lenovo у меня технология уже была включена.

Ручная инициализация AMT



Intel(R) Management Engine BIOS Extension v6.0.3.0010
Copyright(C) 2003-09 Intel Corporation. All Rights Reserved.

Intel(R) ME Firmware version 5.0.0.1184
Press **CTRL-P** to enter Intel(R) ME Setup

29

©2017, ОАО «ИнфоТекс»

В случае ручной инициализации пользователю нужно зайти в Management Engine BIOS Extension, нажав специальную комбинацию клавиш. Обычно это Ctrl+P.

Ручная инициализация AMT

infotecs

```
Intel(R) Management Engine BIOS Extension v6.0.3.8018/Intel(R) ME v6.0.0.1184
Copyright(C) 2003-09 Intel Corporation. All Rights Reserved.
[ MAIN MENU ]
Intel(R) ME General Settings  >
Intel(R) AMT Configuration    >
Intel(R) Quiet System Technology Configuration >
Exit

Intel(R) ME Password
_____

[ESC]=Exit [ENTER]=Submit
```

30

©2017, ОАО «ИнфоТекс»

После этого необходимо задать пароль администратора. Он должен быть не менее 8-и символов, содержать как минимум одну букву нижнего регистра, верхнего регистра, спец. символ и цифру.

Ручная настройка AMT

infotecs

```
Intel(R) Management Engine BIOS Extension v6.0.3.8818/Intel(R) ME v6.0.0.1184
Copyright(C) 2003-09 Intel Corporation. All Rights Reserved.
[ WIRED LAN IPV4 CONFIGURATION ]
  DHCP Mode
  IPV4 Address
  Subnet Mask Address
  Default Gateway Address
  Preferred DNS Address
  Alternate DNS Address
  Previous Menu

[ESC]=Exit      [↑↓]=Select      [ENTER]=Access
```

31

©2017, ОАО «ИнфоТекс»

После этого пользователь может вручную сконфигурировать AMT, например, задать сетевые настройки.

Ручная настройка AMT

infotecs

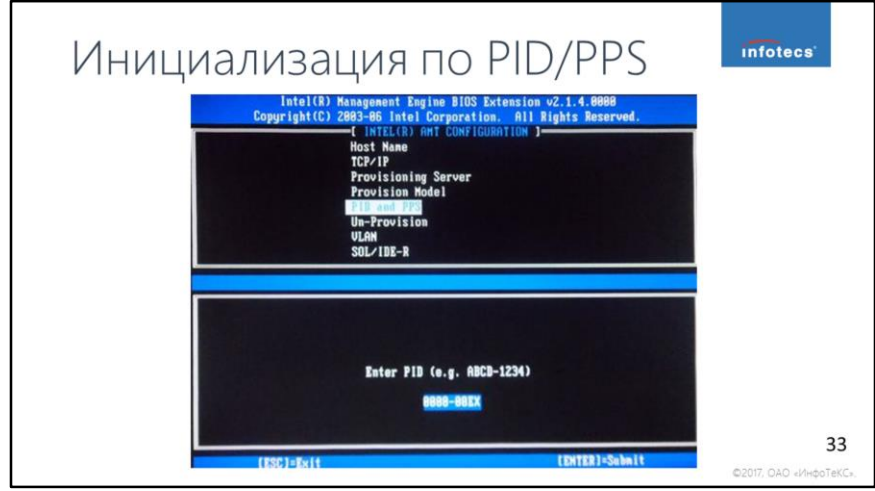


32

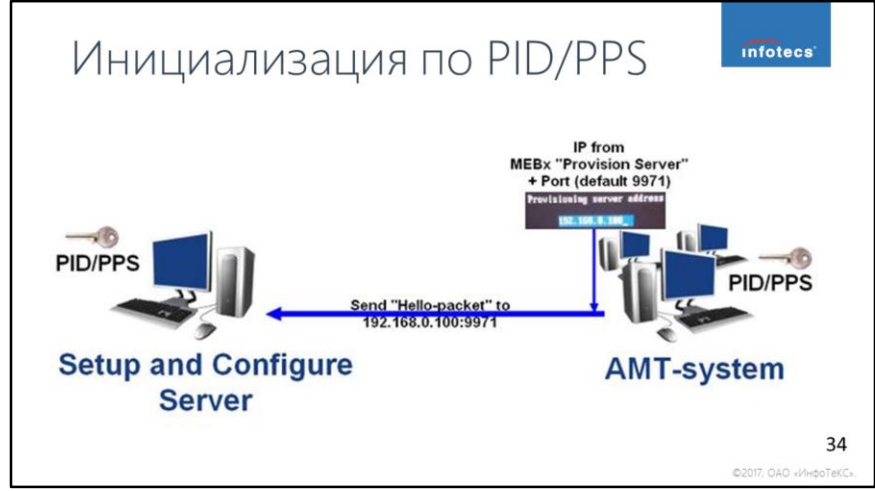
©2017, ОАО «ИнфоТекс»

Или включить функцию KVM.

Ручная конфигурация не подходит, если парк машин достаточно большой.



Теперь рассмотрим инициализацию через Provision ID, PreProvision Secret.
Для того, чтобы отработал PID/PPS вариант инициализации AMT, необходимо, что данная пара "ключей" была и на SCS-сервере (Intel Setup and Configuration Server) и на AMT-компьютере.
Заходим в MEBx, при необходимости устанавливаем новый пароль, в меню "PID and PPS" вводим сначала PID = 0000-00EX, а после PPS=0000-0000-0000-0000-0000-0000-0000-0369.




Как только мы введём последний символ PPS и нажмём ввод, произойдёт следующая череда событий:

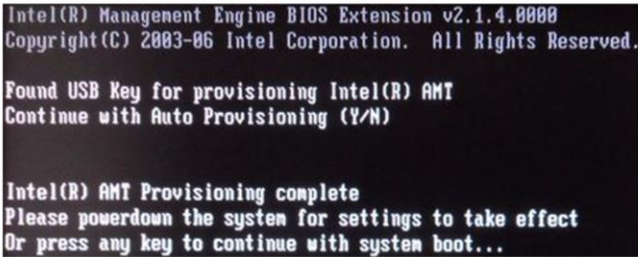
1. AMT отсылает так называемый Hello-packet на Provisioning Server. Это либо заданное значение в MEBx, либо адрес вычисляется следующим образом:
 AMT делает DHCP-запрос и получает поле Option 15 (DNS-suffix). Далее AMT к нему добавляет поддомен "provisionserver", на который и отправляет Hello-packet:
 Одновременно с посылкой Hello-packet, AMT открывает свой порт 16993 (изначально он закрыт по соображениям безопасности)
2. Сервер, получив Hello-packet, запоминает IP, с которого он пришёл. Далее в своей базе находит PPS, который соответствует PID из Hello-packet-a
3. AMT проверяет PPS и если он совпадает с тем, что был сохранён ранее, подтверждает установку шифрованного соединения. На этом инициализация заканчивается и компьютер AMT может быть сконфигурирован по защищённому соединению

Если внимательно присмотреться, мы много действий делали "вручную" - это и первый заход в MEBx, и задание пароля, который после должен попасть на сервер, и задание PID/PPS, тоже нужных серверу для инициализации.

Инициализация через USB



```
USBfile -create setup.bin admin AdmIn.Pass -pid 0000-00EX -pps  
0000-0000-0000-0000-0000-0000-0000-0369 -v 1
```



35

©2017, ОАО «ИнфоТекС»

Потому ещё и в первой версии AMT для облегчения жизни админа AMT привлекли вполне очевидный вариант с использованием USB-флешки, на которую удобно записать из ОС нужные настройки и которые после бы "подхватил" MEBx и ME/AMT.

Так появилась утилита USBFile, которая позволяет сформировать файл "setup.bin". Пример вызова утилиты приведён на слайде.

Файл "setup.bin", будучи помещённым в корень USB-накопителя, отформатированного в FAT16 - автоматически обнаруживается MEBx при загрузке непроинициализированного AMT-компьютера и позволяет автоматически запустить процесс инициализации/конфигурации плюс задать некоторые важные настройки.

Инициализация через Internet

infotecs

1. АМТ-компьютер отправляет Hello-пакет на инициализационный сервер.
Адрес сервера вычисляется как "privosionserver" + Parent Domain (в настройках DHCP).
2. Инициализационный сервер должен иметь специальный сертификат, предназначенный для инициализации vPro-систем, выданный авторизованным Intel для этих целей регистратором.
3. АМТ-компьютер проверяет подлинность сертификата сервера, после чего соглашается на инициализацию и принимает конфигурационные данные с сервера из интернета.

36

©2017, ОАО «ИнфоТекс»

Инициализация через Internet работает в полностью автоматическом режиме:

1. АМТ-компьютер отправляет Hello-пакет на инициализационный сервер. Адрес сервера вычисляется как "privosionserver" + Parent Domain (в настройках DHCP) (или DNS-suffix).
2. Инициализационный сервер должен иметь специальный сертификат, предназначенный для инициализации vPro-систем, выданный авторизованной компанией Intel для этих целей регистратором. root-хэш такого сервера присутствует в хранилище сертификатов АМТ-компьютера.
3. АМТ-компьютер проверяет подлинность сертификата сервера, после чего соглашается на инициализацию и принимает конфигурационные данные с сервера из интернета.

Для примера в сети доступен сервер *vpro.by*, который проинициализирует АМТ и установит пароль "*vPro.by1*".

Demo

Технологии на основе ME



- Active Management Technology
- Anti-Theft Technology
- Identity Protection Technology

38

©2017, ОАО «ИнфоТекс»

Переходим к Anti-Theft Technology

Anti-Theft Technology

Компьютер с технологией AT может быть заблокирован:

1. после ошибки синхронизации с удалённым сервером через заданный интервал времени;
2. если удалённый сервер просигнализирует, что компьютер был украден;
3. через доставку «таблетки с ядом» (через SMS, если есть 3G-модем).



infotecs

39

©2017, ОАО «ИнфоТекС».

Intel приводит статистику, что каждые 53 секунды в мире крадут ноутбук. Anti-Theft Technology предназначена, как и следует из названия, для борьбы с кражами компьютеров.

Компьютер, поддерживающий технологию Intel AT, может быть заблокирован несколькими способами (в случае инициализации процедуры блокировки компьютера система не проходит Power-On-Self-Test):

1. после ошибки синхронизации с удалённым сервером через заданный интервал времени;
2. если удалённый сервер просигнализирует, что компьютер был украден;
3. через доставку «таблетки с ядом» (через SMS, если есть 3G-модем).

В случае блокировки злоумышленникам не удастся запустить ноутбук даже в случае если будет заменён или отформатирован жёсткий диск, предпринята попытка переустановки операционной системы или порядок загрузки накопителя. Технология AT, будучи реализованной на основе ME, полностью блокирует систему на аппаратном уровне и не зависит от основной системы.

Anti-Theft Technology

infotecs

При наличии GPS:

- Можно заранее задать географическую область, за пределами которой ноутбук блокируется.
- В случае кражи компьютера, можно отслеживать его местоположение.

Может инициировать удаление с машины ключей для расшифровки жёсткого диска.

Блокировка является обратимой (через ввод предварительно заданного пароля для разблокировки).

40

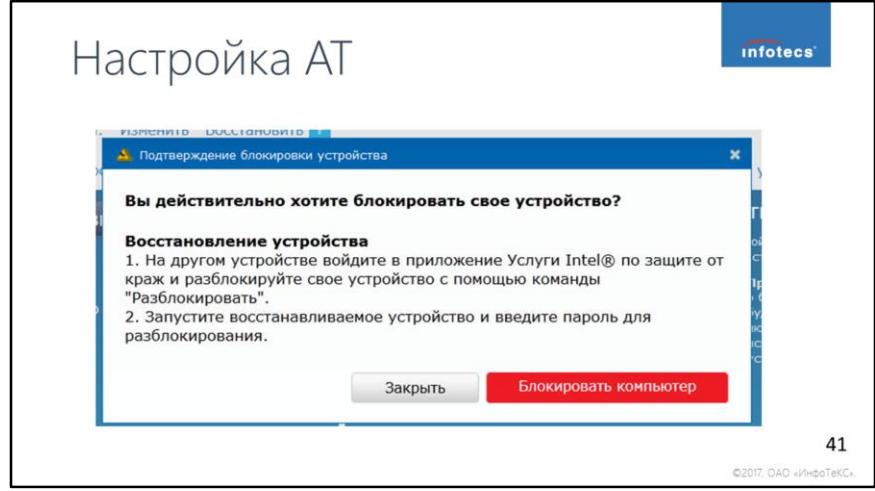
©2017, ОАО «ИнфоТекс»

При наличии GPS:

- Можно заранее задать географическую область, за пределами которой ноутбук блокируется.
- В случае кражи компьютера, можно отслеживать его местоположение.

Может инициировать удаление с машины ключей для расшифровки жёсткого диска.

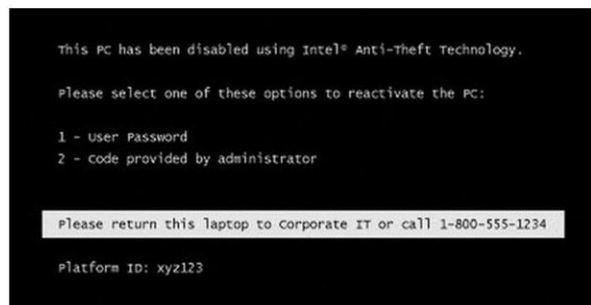
Блокировка является обратимой (через ввод предварительно заданного пароля для разблокировки).



Для активации услуги нужно было зарегистрироваться на сайте ATservice.intel.com и завести учётную запись для каждого из используемого устройств. Затем осуществляется привязка компьютера к аккаунту с помощью специального приложения. После того как компьютер зарегистрирован в системе, пользователь через web-интерфейс может настраивать интервалы «рандеву» с сервером, менять сообщение которое показывается в режиме блокировки и, наконец, в любой момент объявить систему в розыск.

Блокировка загрузки

infotecs



42

©2017, ОАО «ИнфоТекс»

Как только нашедший или злоумышленник попытаются включить заблокированный компьютер, на экране появится сообщение с просьбой вернуть устройство владельцу.

AT discontinued



Intel® Anti-Theft Service FAQ

In an effort to help streamline our security offerings, Intel is winding down its Intel® Anti-Theft Technology business, including its Intel® Anti-Theft Service. **Intel® Anti-Theft Service will be terminated by the end of January, 2015.** If you are a current user of Intel® Anti-Theft Service and your subscription ends after this date, Intel will be contacting you with further information about your subscription. If you are a user of another company's product that relies on Intel® Anti-Theft Technology, please contact the company directly to learn more about its plans. For more information about the termination of Intel® Anti-Theft Service, please see the FAQ.

43

©2017, ОАО «ИнфоТекс»

К сожалению, в 2015-м году Intel отказалась от поддержки этой системы. Сервис больше не функционирует.

Технологии на основе ME



- Active Management Technology
- Anti-Theft Technology
- Identity Protection Technology

44

©2017, ОАО «ИнфоТекс»

Другой технологией, не получившей широкого распространения стала Identity Protection Technology.

Identity Protection Technology

Комплект технологий для аутентификации и онлайн-доступа, предоставляющий пользователям безопасность, основанную на аппаратном обеспечении:

- One Time Password
- Protected Transaction Display


45
©2017, ОАО «ИнфоТекС»

IPT – это бренд, который объединяет несколько технологий для аутентификации и онлайн-доступа, предоставляющий пользователям усиленную безопасность, основанную на аппаратном обеспечении.

Мы рассмотрим две из них:

- One Time Password
- Protected Transaction Display

One Time Password



Intel® Identity Protection Technology with One-Time Password (OTP)

Username, Password + One-Time Password: 927316 = [Server icon]

A one-time password token is built directly into the chipset of select 2nd and all higher-generation Intel® Core™ processors and Intel® Core™ vPro™ processors, enabling seamless two-factor authentication and secure VPN access.

46

©2017, ОАО «ИнфоТекс»

ОТР предназначена для упрощения проведения двухфакторной аутентификации. Обычно в двухфакторной аутентификации используются известные пользователю данные (имя пользователя и пароль) и имеющиеся у пользователя средства аутентификации (обычно токен или электронный ключ). В случае использования одноразового пароля, внешнее средство аутентификации генерирует код, доступный по запросу и действующий в течение короткого периода времени).

One Time Password

infotecs


$$\text{OTP}(\text{key}, \text{time}) := \text{Truncate}(\text{HMAC}(\text{seed}, \text{time}))$$

47

©2017, ОАО «ИнфоТекс»

Примером устройств, генерирующий одноразовый пароль являются токены RSA SecurID. Intel OTP представляет собой встроенный аппаратный токен, который позволяет отказаться от использования отдельных физических токенов и упростить процесс двухфакторной аутентификации. В качестве внешнего устройства, которое используется для получения одноразового пароля выступает подсистема ME, которая фактически изолирована от основной системы. Для использования токена на базе Intel OTP нужно сначала его проинициализировать, снабдив его т.н. **seed**. После чего по запросу можно генерировать одноразовые пароли, которые рассчитываются как функция от **seed** и текущего времени. Принцип работы точно такой же как у аппаратных токенов. И некоторые производители (такие как RDA) портировали свои системы двухфакторной аутентификации на Intel IPT.

Protected Transaction Display



Intel® Identity Protection Technology with Protection Transaction Display

PKI Certificate Or One-Time Password 927316 PIN Pad

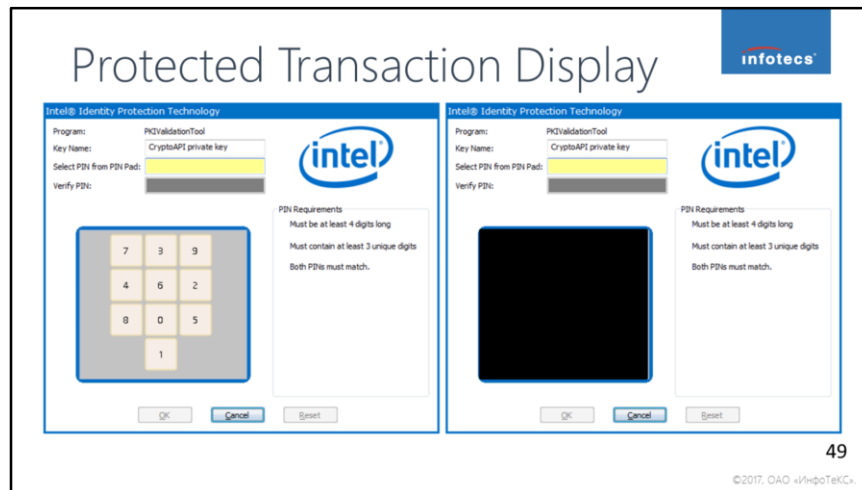
Protects and hides PC display from malware scraping and proves human presence at PC. Secure technology for entering PINs, transaction verification, and ACH fraud prevention.

48

©2017, ОАО «ИнфоТекс»

The diagram illustrates the Protected Transaction Display (PTD) technology. It shows a user at a laptop with an Intel Identity Protection Technology (IPT) icon. The user can authenticate using either a PKI Certificate or a One-Time Password (OTP) displayed on the screen (e.g., 927316). A PIN Pad is also shown as an input method. The technology is connected to a server rack in the cloud. A blue banner at the bottom explains that PTD protects and hides the PC display from malware scraping and proves human presence at the PC, serving as secure technology for entering PINs, transaction verification, and ACH fraud prevention.

Технология Protected Transaction Display (PTD) позволяет отображать информацию для пользователя и получать данные, введенные пользователем, используя подсистему ME для повышения безопасности ввода (например, ввода одноразового пароля). Сделано это следующим образом.



Пользователю для ввода пароля представляется табло с экранной клавиатурой. Эта информация, отображаемая с использованием РТD, видна только пользователям, физически присутствующим перед экраном устройства. Информация внутри табло отображается подсистемой ME, которая имеет выделенный доступ к видеоадаптеру (технологий работает только в случае использования интегрированного графического ядра Intel). Информация не видна основной ОС. Хотя основная ОС может считать нажатия мыши, это не позволит восстановить введенный код, т.к. цифры на экранной клавиатуре располагаются каждый раз случайным образом.

Таким образом, эта возможность помогает свести к минимуму действия вредоносного ПО, считывающего отображенную на экране информацию и регистраторов работы клавиатуры/мыши.

IPT discontinued



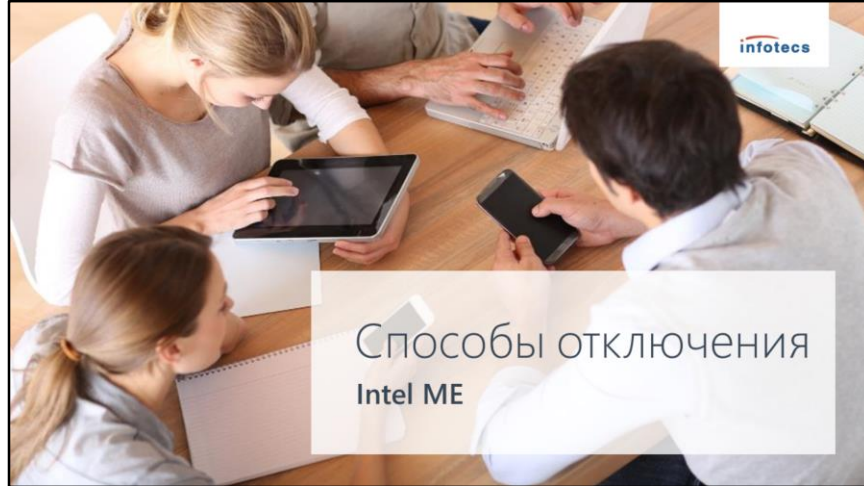
Intel® Identity Protection Technology is discontinued now; it only works with Windows® 7 and 8.0.

<https://communities.intel.com/>

50

©2017, ОАО «ИнфоТекс»

К сожалению, Intel уже прекратила поддержку этой технологии, также как и Anti-Theft.



Способы отключения
Intel ME

ME = backdoor?

infotecs



I could not imagine a more ideal infrastructure for malware than the Management Engine.

©Rutkowska J.

The Intel Management Engine and its applications are a backdoor with total access to and control over the rest of the PC. The ME is a threat to freedom, security, and privacy.

©libreboot project

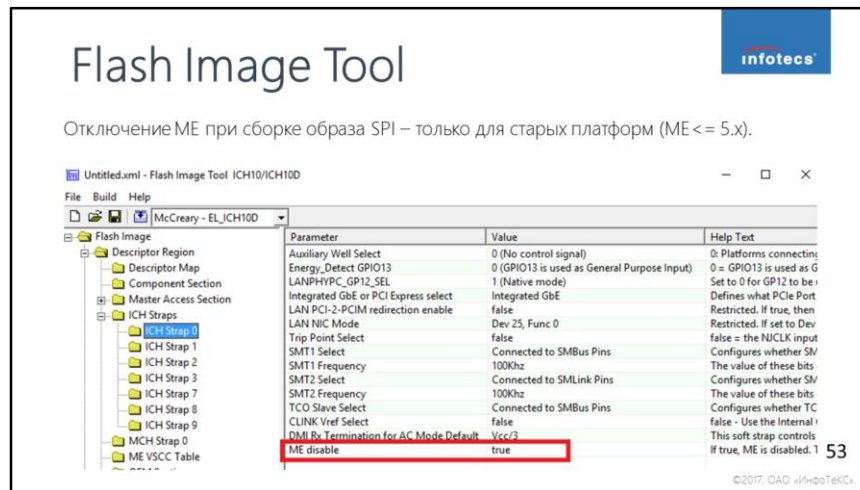
52

©2017, ОАО «ИнфоТекс»

Имея столь широкие полномочия, подсистема ME была воспринята многими как бэкдор в чипсете. Люди начали искать способы отключения ME.

При этом важно отметить, что не обязательно сама ME может быть вредоносной и содержать backdoor. В ME могут быть баги или уязвимости, которые потребители никак исправить не смогут.

Например, команда Invisible Things Lab уже продемонстрировала способ компрометации ME.



На старых платформах (Intel ME версии 5.x и ниже) выключить данную подсистему можно, воспользовавшись Flash Image Tool (утилита из Intel System Tool Kit , предназначенная для сборки образов SPI флэш-памяти из отдельно взятых регионов BIOS, ME, GbE). При сборке задаются параметры, которые прописываются в этих регионах и в регионе Flash Descriptors. В последнем есть флаг «ME disable». Способ считается безопасным, но работает только на старых платформах.

Intel System Tool Kit (STK) — комплект программных средств и документации для сборки образов SPI флэш-памяти, применения этих образов и получении информации о текущем состоянии Intel ME.

Flash Image Tool

infotecs

Временное отключение через MEI на новых платформах (ME >= 9.x).

```
Administrator: Command Prompt
D:\intel me\Intel ME System Tools v9.0 r2\Flash Programming Tool\WINDOWS64>fptw64.exe -disableme

Intel (R) Flash Programming Tool. Version: 9.0.22.1467
Copyright (c) 2007 - 2013, Intel Corporation. All rights reserved.

Platform: Intel(R) B85 Express Chipset
Reading HSFSTS register... Flash Descriptor: Valid

--- Flash Devices Found ---
MX25L6405D  ID:0xC22017  Size: 8192KB (65536Kb)

The ME is disabled.
FPT Operation Passed

D:\intel me\Intel ME System Tools v9.0 r2\Flash Programming Tool\WINDOWS64>
```

54

©2017, ОАО «ИнфоТекС»

На новых платформах (начиная с Intel ME 9 версии), в утилиту Flash Programming Tool, предназначенную для программирования SPI флэш-памяти компьютерных платформ, была добавлена возможность временно выключать Intel ME. Выключение выполняется отправкой команды в MEI. Согласно документации, в таком состоянии подсистема Intel ME находится до следующего запуска компьютера или перезагрузки.

Нельзя говорить о том, что этот способ позволяет полностью отключить Intel ME, хотя бы потому, что до момента принятия команды на отключение ME-контроллер успеет загрузиться, а значит, выполнить некоторую часть кода прошивки. Несмотря на то, что Intel ME не подаёт «признаков жизни» после этой операции, неизвестно, может ли эту подсистему заново включить какой-нибудь сигнал извне. Также неясно, насколько Intel ME выключена.

Обнуление SPI-региона ME

Home / Laptops / Libreboot X220 *PREORDER*

Libreboot X220 *PREORDER*

£798.00-£1,198.00

Storage and RAM
8GB RAM and 160GB HDD
Clear selection

£898.00

In stock

1 | Add to cart

Cart
No products in the cart.

infotecs

55

©2017, ОАО «ИнфоТекС»

Поскольку прошивка ME хранится на SPI-памяти, можно попробовать просто обнулить регион ME в надежде, что система не найдёт прошивку и таким образом отключится.

Так, в частности, попробовали сделать разработчики т.к. ноутбуков Libreboot. Это ноутбуки на базе Lenovo Thinkpad, но в которых в качестве BIOS используется coreboot.

Обнуление SPI-региона ME



Before version 6.0, the ME can be disabled by setting a couple of values in the SPI flash memory. The ME firmware can then be removed entirely from the flash memory space. ME firmware versions 6.0 and later include "ME Ignition" firmware that performs some hardware initialization and power management. If the ME's boot ROM does not find in the SPI flash memory an ME firmware manifest with a valid Intel signature, the whole PC will shut down after 30 minutes.

56

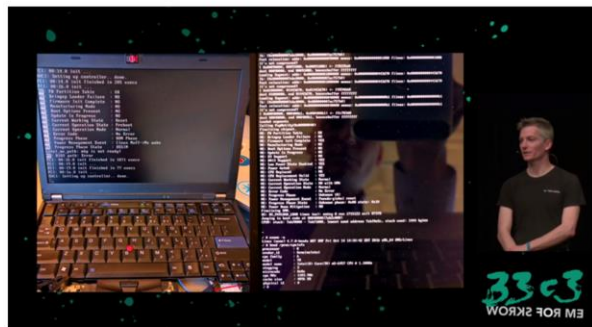
©2017, ОАО «ИфоТекС»

В результате их платформа либо вовсе не загружалась без наличия подлинной прошивки ME, либо выключалась ровно после 30 минут работы.

Отказ компьютерной системы грузиться без прошивки Intel ME можно объяснить важностью ME-контроллера в процессе инициализации аппаратной составляющей. А 30-минутный таймаут наводит на мысль о WDT (Watch Dog Timer).

Урезание прошивки ME

infotecs



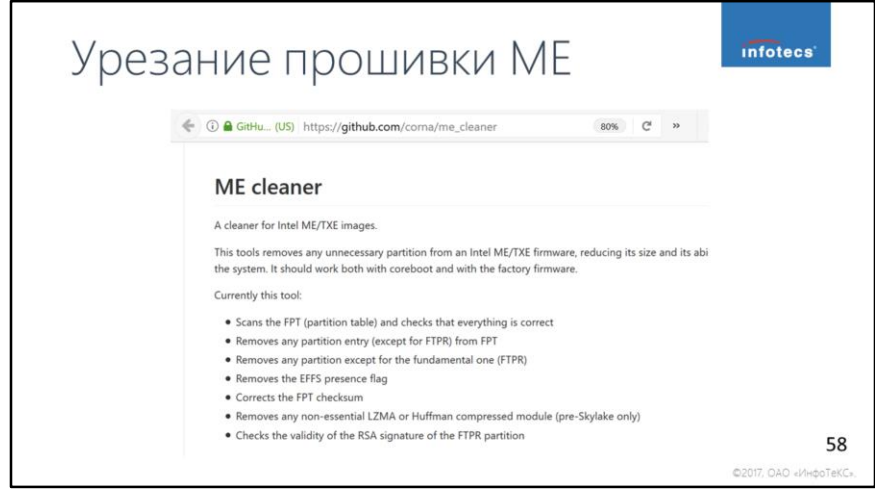
T. Hudson:
Bootstrapping a
slightly more
secure laptop

57

©2017, ОАО «ИнфоТекс»

Несколько дальше в этом направлении продвинулся Трэмелл Хадсон. На последней конференции С3 он продемонстрировал возможность урезания прошивки ME с 5-и Мб до 41Кб. Это нельзя считать полным успехом, т.к. часть прошивки всё же остаётся и не понятно что именно она делает. Но функциональность ME от этого определённо снижается.

Урезание прошивки ME



The screenshot shows a web browser window displaying the GitHub repository page for 'me_cleaner' by user 'coma'. The browser's address bar shows the URL 'https://github.com/coma/me_cleaner'. The page title is 'ME cleaner'. Below the title, there is a description: 'A cleaner for Intel ME/TXE images. This tool removes any unnecessary partition from an Intel ME/TXE firmware, reducing its size and its ABI the system. It should work both with coreboot and with the factory firmware. Currently this tool:' followed by a bulleted list of features: 'Scans the FPT (partition table) and checks that everything is correct', 'Removes any partition entry (except for FTFR) from FPT', 'Removes any partition except for the fundamental one (FTFR)', 'Removes the EFS presence flag', 'Corrects the FPT checksum', 'Removes any non-essential LZMA or Huffman compressed module (pre-Skylake only)', and 'Checks the validity of the RSA signature of the FTFR partition'. The number '58' is visible in the bottom right corner of the screenshot area, and a copyright notice '©2017, ОАО «ИнфоТекс»' is at the very bottom.

infotecs

← GitHub... (US) https://github.com/coma/me_cleaner 80% ↻ »

ME cleaner

A cleaner for Intel ME/TXE images.

This tool removes any unnecessary partition from an Intel ME/TXE firmware, reducing its size and its ABI the system. It should work both with coreboot and with the factory firmware.

Currently this tool:

- Scans the FPT (partition table) and checks that everything is correct
- Removes any partition entry (except for FTFR) from FPT
- Removes any partition except for the fundamental one (FTFR)
- Removes the EFS presence flag
- Corrects the FPT checksum
- Removes any non-essential LZMA or Huffman compressed module (pre-Skylake only)
- Checks the validity of the RSA signature of the FTFR partition

58

©2017, ОАО «ИнфоТекс»

Утилита для урезания региона ME свободно доступна на GitHub.

Не дескрипторный режим SPI



Включение не дескрипторного режима SPI-памяти.

-> ME-контроллер не получит доступ к своему региону, не будет исполнять прошивку.

Нет информации о результатах апробации этого варианта.

59

©2017, ОАО «ИнфоТекС»

Ещё одна теоретическая возможность отключения ME через модификацию SPI заключается во включении т.н. не дескрипторного режима SPI-памяти (т.е. когда в ней содержится только BIOS). В этом случае, ME-контроллер не получит доступ к своему региону, и, следовательно, не будет исполнять прошивку. С одной стороны, ME-контроллер так же, как и в предыдущем случае, может препятствовать нормальной работе компьютерной системы. Этот режим используется вендорами в отладочных целях, поэтому есть шанс, что система запустится. Я пока не нашёл информации о результатах апробации такого режима, только самое предложение.

Удаление ME UMA

infotecs

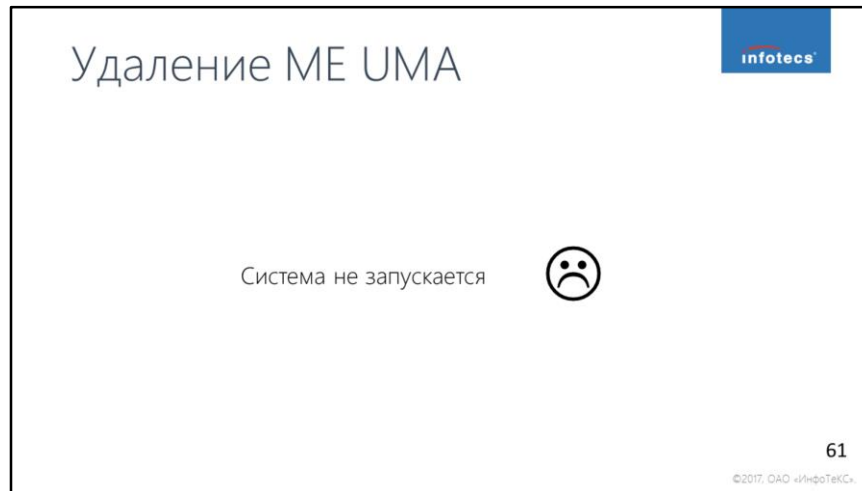
Изменить карту памяти в BIOS, убрав область ME UMA.

->Прошивку ME некуда будет распаковывать, она не будет исполняться.

60



©2017, ОАО «ИнфоТекс»

Известно, что прошивка Intel ME распаковывается в выделенную и скрытую от основного CPU область оперативной памяти – ME UMA. Выделение и блокировку этой области осуществляет BIOS во время конфигурирования карты памяти. Тогда почему бы не вырезать эти фрагменты кода из BIOS, чтобы данная область не выделялась. Тогда прошивка ME не будет распаковываться и исполняться.



Ребята из Digital Security провели такие эксперименты. Они показали, что такой способ не годится, и система не запускается.

Stateless laptop

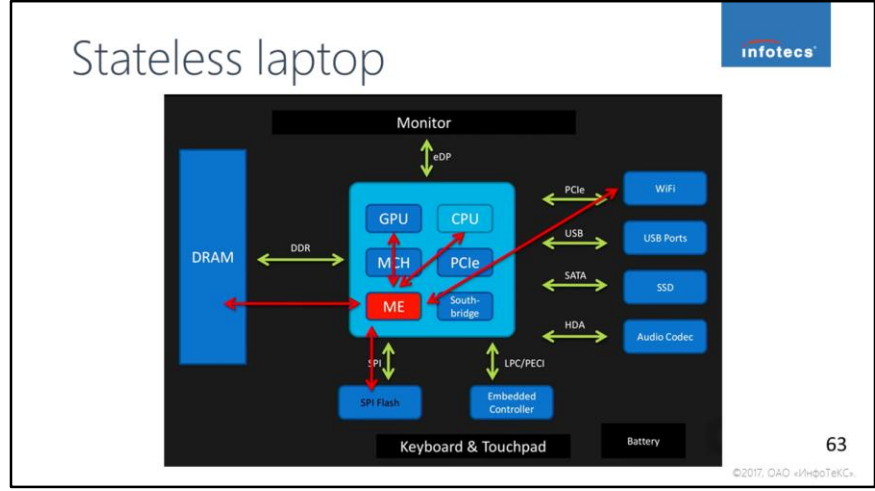


J. Rutkowska: Towards (reasonably) trustworthy x86 laptops

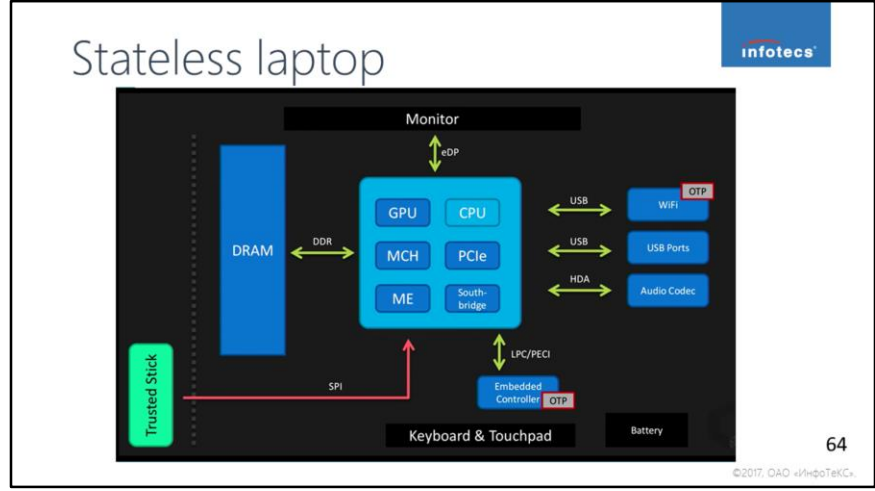
62

©2017, ОАО «ИнфоТекС»

Несколько более творчески подошла к проблеме ME Йоанна Рутковская. Это специалист и исследователь в области компьютерной безопасности. Известна в первую очередь как автор ОС Qubes. На предпоследней конференции СЗ она представила своё видение решения – концепцию т.н. Stateless laptop – т.к. ноутбук без состояния.



Для пояснение сути концепции stateless laptop, рассмотрим сначала схему обычного x86-ноутбука. В центре мы видим микроконтроллер ME, связи которого с другими подсистемами обозначены красными стрелками: он имеет доступ к оперативной памяти, сетевым адаптерам, SPI и т.п.



Тогда минимальная схема Stateless laptop будет выглядеть следующим образом. Добавляется новый элемент системы – Trusted stick, который замещает собой SPI-память и реализует её интерфейс. Этот элемент содержит в себе

- Прошивки (ME, BIOS) и ОС в режиме read-only. Т.е. при попытках перезаписать эту информацию подсистемой ME или кем-то ещё, Trusted stick не позволит этому случиться.
- Зашифрованный пользовательский раздел данных и его ключ. Эти данные доступны в т.ч. в режиме записи.

При этом из схемы пропал накопитель и все прочие прошивки в системе стали на основе OTP (One-Time Programmable) памяти.

Таким образом, суть защиты сводится к тому, чтобы лишить ME возможности сохранять данные где бы то ни было в системе. Если ME и получит доступ к каким-то пользовательским данным, она не сможет их сохранить нигде кроме зашифрованного пользовательского, доступ к которому имеет только пользователь.

Stateless laptop

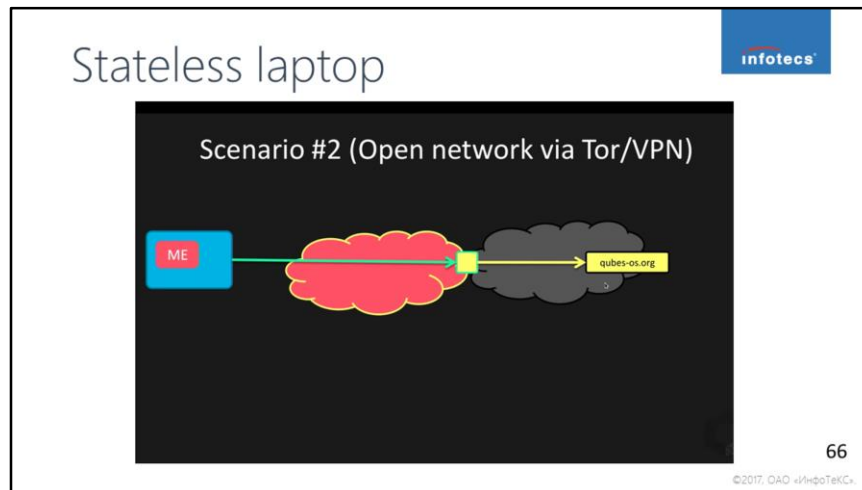
infotecs

Scenario #1 (Closed network of trusted nodes)

65

© 2017, ОАО «ИнфоТекс»

Однако, остаётся возможность утечки пользовательских данных через сеть. Для решения этой проблемы предлагается ввести ещё один элемент – прокси для сетевого адаптера. Прокси должен выступать посредником между CPU и самим адаптером и строить туннель для передачи всех данных (VPN, Tor). В этом случае можно построить защищённую сеть между такими Stateless laptop-ами и без доступа во внешнюю сеть.




При наличии доступа во внешнюю сеть пользовательские данные смогут утечь через этот туннель, но у получателя будут сложности с определением источника. Таким образом, это увеличивает сложность эксплуатации по сравнению, что мы имеем с ME по умолчанию, но не избавляет от проблемы как таковой.

Всякие экзотические каналы утечек типа флуктуаций потребляемой мощности или мигания светодиодами не рассматриваются.

Stateless laptop

В итоге:

- Требует аппаратной модификации (Trusted Stick, Open SSD).
- Вносит ограничения на систему (необходимо шифровать пользовательские данные, ОС в режиме r/o).
- Не решает в полной мере проблему с утечкой данных через сеть.

Отключение ME - итоги 

Lost war?

Since recent versions of it [ME] can't be removed, this means avoiding all recent generations of Intel hardware.

©libreboot project

68

©2017, ОАО «ИнфоТекс»

Подводя итоги рассмотренным способам отключения ME, можно сказать следующее. Некоторые предложенные решения влекут за собой неработоспособность компьютерной системы, другие - не дают гарантии того, что подсистема Intel ME действительно выключена или «обезврежена», как в случае со Stateless Laptop. В связи с этим, вопрос о том, как отключить Intel ME на современных системах остаётся открытым.



Спасибо.
Вопросы?

infotecs